Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)
Organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014, e notificato, ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma elettronica e di un sigillo elettronico qualificati ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento.

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche e di Sigilli Elettronici qualificati ai Requisiti di Sicurezza Previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Attestato di Conformità n. 2/24

Dispositivo: **Trident, the distributed remote Qualified Signature Creation Device version 3.1.3**

Sviluppato da: **I4P-Informatikai Kft. (I4P Informatics Ltd.)**

Il dispositivo per la creazione di firme elettroniche e di sigilli elettronici qualificati indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

Firmato digitalmente da:
Andrea Billet
Data: 10/05/2024 13:02:19

Roma, 10 maggio 2024

Il presente Attestato di Conformità è stato emesso dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) in conformità al comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", modificato ed integrato dal DL 26 agosto 2016, n. 179.
La validità del presente Attestato di Conformità è soggetta alle condizioni e alle ipotesi esplicitate nel Rapporto di Accertamento (OCSI/ACC/NXP/01/2023/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Rapporto di Accertamento

Trident, the distributed remote Qualified Signature Creation Device version 3.1.3

OCSI/ACC/I4P/02/2024/RA

Versione 1.1

10 maggio 2024

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	07/05/2024
1.1	OCSI	Seconda emissione	10/05/2024

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CM	Cryptographic Module
DL	Decreto Legge
QSCD	distributed remote Qualified Signature Creation Device
EAL	Evaluation Assurance Level
ECA	External Client Application
eIDAS	electronic IDentification Authentication and Signature
EN	European Norm
ETSI	European Telecommunications Standards Institute
JWT	JSON Web Token
LCA	Local Client Application
MPCA	Multi-Party Cryptographic Appliance
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PP	Profilo di Protezione
QSCD	Qualified Signature Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SFR	Security Functional Requirement
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TOTP	Time-based One-Time Password (algorithm)
TSF	TOE Security Functions
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179, G.U. n. 214 del 13 settembre 2016

[eIDAS] “Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014

[ESI-CS] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.4.2 (2022-02)

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019

[PR] “Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall’Allegato II al Regolamento (UE) n. 910/2014”, OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016

[RA] “Rapporto di Accertamento Trident version 2.1.3”, OCSI/ACC/I4P/02/2020/RA, Versione 1.0, 22 settembre 2020

[RC] “Rapporto di Certificazione Trident, the distributed remote Qualified Signature Creation Device version 3.1.3”, OCSI/CERT/CCL/14/2022/RC, Versione 1.0, 16 aprile 2024

[TDS] “Trident, the distributed remote Qualified Signature Creation Device” Security Target, v3.5, I4P-informatikai Kft., 16 January 2024

5 Ambito dell'Accertamento di Conformità

L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014 sull'identità digitale – eIDAS (*Electronic IDentification, Authentication and Signature*) [eIDAS] e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica e di un sigillo elettronico qualificati ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento (UE) n. 910/2014.

L'affidamento all'OCSI dell'accertamento di cui sopra è specificato dal comma 5 dell'articolo 35 del d.lgs. 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" [CAD], modificato ed integrato dal DL 26 agosto 2016, n. 179.

L'Accertamento è stato condotto dall'OCSI in accordo a quanto indicato nella "Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014", OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016 [PR] (nel seguito indicata come Procedura).

L'oggetto dell'Accertamento di Conformità è il dispositivo denominato "Trident, the distributed remote Qualified Signature Creation Device v3.1.3", sviluppato dalla società I4P-informatikai Kft. (I4P Informatics Ltd.) (nel seguito indicato anche come "Trident version 3.1.3" o "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo")

Il dispositivo oggetto dell'Accertamento è un **Dispositivo di Tipo 2**, così come definito nel cap. 6, punto A.ii, della Procedura.

Il dispositivo comprende un applicativo software (componente SAM), certificato in conformità con il Profilo di Protezione (PP) EN 419241-2:2019 [PP-SAM], e un modulo crittografico (componente CM), certificato in conformità con il PP EN 419221-5:2018 [PP-CM].

L'insieme dei due componenti SAM e CM costituisce il dispositivo sicuro per la creazione di firme elettroniche qualificate e sigilli elettronici qualificati (QSCD) conforme al Regolamento (UE) n. 910/2014 [eIDAS].

Si noti che il dispositivo oggetto dell'Accertamento è una versione aggiornata del dispositivo denominato "Trident version 2.1.3", già accertato dall'OCSI (Attestato di Conformità n. 2/20 del 22 settembre 2020 [RA]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore è stato necessario procedere a una ri-certificazione dell'ODV, i cui risultati sono riportati nel Rapporto di Certificazione [RC].

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente dispositivo, per facilità di lettura il presente Rapporto di Accertamento è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo dispositivo "Trident version 3.1.3".

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo, prodotto dalla società I4P-informatikai Kft. (I4P Informatics Ltd.), ed è finalizzato a fornire indicazioni ai potenziali acquirenti ed utilizzatori di tale dispositivo circa la sua conformità ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per la creazione di una firma elettronica e di un sigillo elettronico qualificati.

Il dispositivo oggetto dell'Accertamento, così come descritto nel relativo Traguardo di Sicurezza [TDS] è risultato conforme ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura per i Dispositivi di Tipo 2 (cap. 7, punto B) e può quindi essere utilizzato sia per la creazione di una firma elettronica qualificata (*qualified electronic signature creation device*), sia per la creazione di un sigillo elettronico qualificato (*qualified electronic seal creation device*).

Il presente Rapporto di Accertamento deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto e al relativo Rapporto di Certificazione [RC].

La validità dell'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento è soggetta alle condizioni e alle ipotesi esplicitate nel presente Rapporto di Accertamento (vedi cap. 7), che ne costituisce parte integrante e sostanziale.

Il rilascio dell'Attestato di Conformità da parte dell'OCSI non rappresenta alcun tipo di sostegno o promozione all'uso del dispositivo accertato da parte di questo Organismo.

6.2 Descrizione del dispositivo accertato

Il dispositivo "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3" è un dispositivo multi-utente e multi-chiave, progettato per essere utilizzato come QSCD composto da un Modulo Crittografico (CM, Cryptographic Module) e da un Modulo di attivazione della firma (SAM, Signature Activation Module) ed è adatto all'uso sia in locale, sia da remoto.

Il dispositivo costituisce parte dell'infrastruttura di un sistema affidabile che supporta la firma lato server (TW4S) e offre servizi di firma elettronica da remoto, garantendo che le chiavi di sottoscrizione del Firmatario vengano utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.
A seconda della sua configurazione, il dispositivo certificato (ODV) è costituito da una, o più componenti MPCA (*Multi-Party Cryptographic Appliance*). Una MPCA si presenta sotto forma di apparato con chassis metallico, montabile su rack.

Nella configurazione denominata **Distributed Configuration** (configurazione distribuita), l'ODV è composto da n (con n = 2, 3 o 4) componenti MPCA identiche che operano come una sola unità logica che, nel suo insieme, soddisfa i requisiti del Traguardo di Sicurezza [TDS]. Nel caso in cui alcune delle MPCA dovessero smettere di funzionare (ad es., a causa di un errore non recuperabile o per l'indisponibilità della rete), le eventuali MPCA rimaste sono in grado di garantire una funzionalità limitata.

Nel caso di **configurazione High-availability** (ad alta affidabilità), l'ODV è costituito invece da una o più istanze completamente ridondate di un nodo attivo (Online) MPCA, ciascuna delle quali sono portate nello stato online quando il nodo attivo ha un malfunzionamento.

Il dispositivo certificato (ODV) è formato da due componenti principali, situati all'interno dell'involucro fisico di una MPCA, che operano congiuntamente per soddisfare diversi insiemi di requisiti:

- il componente **Cryptographic Module (CM)** è un **modulo crittografico** di uso generico che fornisce il supporto crittografico necessario per i suoi utenti legittimi (service provider che supportano le operazioni sia relative alla firma locale o remota sia relative all'apposizione di un sigillo elettronico, l'emissione e la revoca di certificati, l'apposizione di marcature temporali e i servizi di autenticazione). L'ODV può anche essere configurato per generare, memorizzare ed attivare la chiave del firmatario in uno o più CM esterni per migliorare le prestazioni o per motivi di retrocompatibilità;
- il componente **Signature Activation Module (SAM)** è un'applicazione locale installata all'interno del perimetro protetto da manomissione dell'ODV che implementa il Signature Activation Protocol (SAP). Il SAM utilizza i Signature Activation Data (SAD) di un firmatario remoto per attivare la chiave di sottoscrizione corrispondente da utilizzare all'interno di un modulo crittografico.

Il modulo CM mantiene l'amministratore, l'utente delle chiavi, i ruoli LCA ed ECA e l'associazione degli utenti ai ruoli. Il CM utilizza per ciascun ruolo un metodo comune per l'identificazione e l'autenticazione: un identificatore univoco e una password statica e/o TOTP (Time-based-One-Time Password) e/o un JWT (JSON Web Token). Prima di utilizzare una chiave segreta è necessaria un'autorizzazione o una ri-autorizzazione. Il CM blocca l'account/la chiave dopo un numero predefinito di tentativi consecutivi di autenticazione/autorizzazione falliti.

Il CM implementa le seguenti funzioni di sicurezza relative all'intero ciclo di vita delle chiavi:

- importazione delle chiavi;
- generazione delle chiavi;
- ripristino delle chiavi da un backup;
- associazione di un insieme di attributi alle chiavi;
- memorizzazione;
- esportazione delle chiavi;
- utilizzo delle chiavi;
- backup delle chiavi;
- distruzione delle chiavi.

IL CM implementa le seguenti funzioni gestionali:

L'Amministratore può:

- sbloccare un account utente bloccato o una chiave bloccata;
- specificare un valore iniziale alternativo per l'attributo di sicurezza "Utilizzo chiave"; impostando il suo valore su "Generale" o su "Firma";
- esportare ed eliminare il file di registro locale degli errori e di controllo;

- eseguire il backup e ripristino dello stato delle funzioni di sicurezza dell'OdV (FSO) del CM.

L'utente della chiave può modificare i seguenti attributi della propria chiave:

- dati di autorizzazione;
- flag Non Protetto (che indica se la sua chiave memorizzata è protetta solo con una chiave infrastrutturale, oppure in aggiunta con i suoi dati di autorizzazione.);
- flag operativo (che indica se la chiave è in stato operativo).

Il SAM non esegue operazioni di crittografia con la chiave dell'utente *Key User* e non elimina la chiave di tale utente. Il SAM invoca invece il CM con parametri appropriati ogni volta che è richiesta un'operazione crittografica, una generazione di chiavi o una cancellazione di chiavi. Allo stesso tempo SAM esegue operazioni crittografiche *non distribuite* con chiavi infrastrutturali.

Il SAM mantiene i ruoli Utenti privilegiati e Firmatario. Il SAM garantisce che tutti gli utenti abbiano un solo ruolo, di conseguenza un firmatario non può essere un utente privilegiato. Per il firmatario, il SAM richiede due diversi fattori di autenticazione, una password e un TOTP o un JWT. Il metodo di identificazione e autenticazione è: identificativo utente univoco + password statica + TOTP o JWT. Il SAM blocca l'account dopo un numero predefinito di tentativi di autenticazione consecutivi non riusciti. Quando l'account del firmatario è stato bloccato, il SAM sospende anche l'utilizzo di tutte le chiavi di firma del firmatario. Il SAM mantiene gli account (con diversi attributi di sicurezza) appartenenti ai singoli utenti.

Il SAM implementa le seguenti funzioni gestionali:

- Gestione dei firmatari
- Gestione degli Utenti Privilegiati
- Gestione della configurazione
- Funzioni di backup e ripristino

6.2.1 Configurazione valutata dell'ODV

La configurazione certificata del dispositivo "Trident version 3.1.3" include i seguenti elementi:

- una, due, tre, quattro MPCA (ODV);
- la documentazione di guida, che fornisce informazioni sulla configurazione certificata e consente di installare e utilizzare correttamente il dispositivo.

Maggiori dettagli sono inclusi nel cap. 1.4 (TOE Description) del Traguardo di Sicurezza [TDS] e nel cap. 10 (Appendice B - Configurazione valutata) del Rapporto di Certificazione [RC].

Il dispositivo è risultato conforme ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], a condizione che vengano rispettate le prescrizioni per l'utilizzo del dispositivo indicate nel cap. 8 del presente Rapporto di Accertamento.

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	I4P-informatikai Kft. (I4P Informatics Ltd.)
Nome del dispositivo	Trident version v3.1.3
Versione del dispositivo	V3.1.3
Traguardo di Sicurezza	“Trident, the distributed remote Qualified Signature Creation Device” Security Target, v3.5, I4P-informatikai Kft., 16 January 2024 ([TDS])
Livello di garanzia	EAL4 con l’aggiunta di AVA_VAN.5 e ALC_FLR.3
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419221-5:2018 ([PP-CM]) EN 419241-2:2019 ([PP-SAM])
Data di inizio della Procedura	9 aprile 2024
Data di rilascio Certificato CC	16 aprile 2024
Data di rilascio Accertamento	10 maggio 2024

7 Condizioni di validità dell'Attestato di Conformità

L'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento deve essere ritenuto valido ed efficace unicamente sotto le seguenti ipotesi:

i. la certificazione di sicurezza ottenuta ([RC]) è in corso di validità, ovvero il Certificato non è scaduto o non è stato revocato;

ii. il dispositivo reale è conforme a quello certificato e descritto nel TDS;

iii. l'ambiente di utilizzo reale del dispositivo è conforme a quello descritto nel TDS;

iv. sono rispettate tutte le condizioni aggiuntive di utilizzo del dispositivo riportate nel cap. 8 del presente Rapporto di Accertamento.

La violazione dell'ipotesi (i) comporta la perdita di validità dell'Attestato di Conformità.

La violazione di una o più delle ipotesi (ii), (iii) e (iv) ha come conseguenza la perdita di efficacia dell'Attestato di Conformità, che mantiene comunque la sua validità.

Eventuali situazioni che comportino la perdita di validità del presente Attestato di Conformità, siano esse rilevate direttamente dall'Organismo di Certificazione emettitore (OCSI) o portate a conoscenza di quest'ultimo da soggetti esterni, saranno rese note ai soggetti interessati attraverso il sito web dell'Organismo stesso o altri canali ufficiali.

8 Condizioni di utilizzo del dispositivo accertato

Il dispositivo deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS], nel Rapporto di Certificazione [RC] e nella documentazione di guida fornita con l'ODV.

In particolare, la consegna, l'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo devono avvenire in accordo agli obiettivi di sicurezza indicati in [TDS].

Il dispositivo deve essere configurato seguendo scrupolosamente la documentazione di guida inclusa con l'ODV.

Inoltre, per quanto riguarda l'uso del dispositivo in conformità ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014 [eIDAS], nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], si raccomanda di porre particolare attenzione agli aspetti di seguito descritti.

8.1 Limitazioni alla configurazione certificata

La certificazione CC del dispositivo Trident version 3.1.3 comprende per il CM sia il caso d'uso "Local Signing", sia quello "Remote Server Signing", così come descritti nel Profilo di Protezione [PP-CM].

A questo riguardo si precisa che il presente Attestato di Conformità copre unicamente il caso d'uso "Remoto", illustrato in Figura 1.

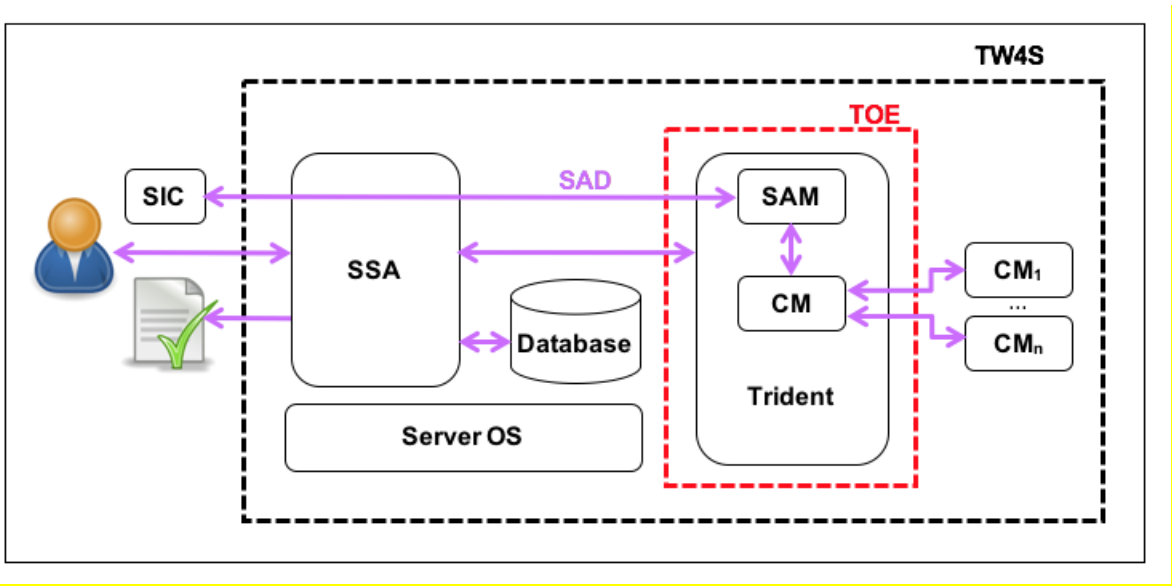

Figura 1 – Il dispositivo Trident version 3.1.3 nel caso d'uso "Remoto"

Questa modalità di utilizzo è rivolta ai TSP che soddisfano i requisiti per la creazione di firme o di sigilli elettronici da remoto, come specificato in [eIDAS]. In questo caso, il CM integrato e la funzionalità SAM del QSCD soddisfano complessivamente i requisiti per i QSCD nel contesto della firma remota, così come descritti nell'Allegato II ad [eIDAS].

Inoltre, per poter essere utilizzato come QSCD, il dispositivo deve essere opportunamente configurato per utilizzare, assieme al modulo SAM, esclusivamente il componente CM integrato in ogni MPCA.

Solamente i due componenti SAM e CM integrato soddisfano complessivamente i requisiti per i QSCD nel contesto della firma remota, così come descritti nell'Allegato II ad [eIDAS]. L'uso di CM esterni, pur contemplato dalla certificazione, non rientra tra le configurazioni coperte dal presente Attestato di Conformità.

8.2 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza (si veda [TDS] par. 1.4.2.1 - CM functionality), nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - Cryptographic Support (si veda [TDS], par. 6.1.2.2).

Per quanto riguarda la generazione di coppie di chiavi crittografiche e i metodi di sottoscrizione, debbono essere utilizzati esclusivamente algoritmi crittografici, lunghezze di chiavi, funzioni *hash*, protocolli e parametri conformi alla specifica ETSI TS 119 312 [ESI-CS].

In generale, per la scelta dei parametri di sicurezza relativi ai metodi di sottoscrizione va tenuto conto di quanto indicato in [ESI-CS], cap 8.3 (*Hash functions versus time*) e cap. 8.4 (*Recommended key sizes versus time*).